2013년 9월 전자공학회 논문지 제 50 권 제 9 호
Journal of The Institute of Electronics Engineers of Korea Vol. 50, NO. 9, September 2013 http://dx.doi.org/10.5573/ieek.2013.50.9.021

논문 2013-50-9-3

# 비단조 접근 구조를 갖는 CP-ABE 방식

# ( Ciphertext Policy-Attribute Based Encryption with Non Monotonic Access Structures )

리프키 사디킨[*], 문 상 재[**], 박 영 호[***]

( Rifki Sadikin, SangJae Moon, and YoungHo Park[ⓒ] )

## 요 약

CP-ABE 방식은 신뢰된 서버 없이 접근 제어 메카니즘을 구현할 수 있다. 본 논문에서는 권한을 부여받은 사용자가 민감한 데이터에 접근할 수 있도록 CP-ABE 방식으로 속성기반 접근 제어 메카니즘을 제안한다. CP-ABE 개념은 암호문에서 접근 제어 방법을 포함하는 것이다. 만약 사용자가 암호문의 접근 구조를 통해 속성을 가진다면 암호문은 복호될 수 있다. 본 논문에서는 제안한 CP-ABE 방식이 비단조 접근 구조로 표현됨을 증명하고 다른 CP-ABE 방식들과 성능 비교한다.

## Abstract

A ciphertext policy-attribute based encryption(CP-ABE) scheme can be used to realize access control mechanism without a trusted server. We propose an attribute-based access control mechanism by incorporating a CP-ABE scheme to ensure only authorized users can access the sensitive data. The idea of CP-ABE is to include access control policy in the ciphertexts, in which they can only be decrypted if a user possesses attributes that pass through the ciphertext's access structure. In this paper, we prove a secure CP-ABE scheme where the policy can be expressed in non-monotonic access structures. We further compare the performance of our scheme with the existing CP-ABE schemes.

**Keywords** : ciphertext-policy attribute based encryption, public key encryption, access control

## Ⅰ. Introduction

Access control is a major issue for deploying a distributed file system over an open network. Traditional user control mechanism keeps user authority in a table usually as a group or in hierarchical structure in an access control list, and then adds access control attribute to a file using a trusted server for authentication and authorization. However, this traditional approach heavily depends on security of the access control list which located in a trusted server. Once the trusted server is compromised then the access control service is also compromised.

There are well known access control models so far: discretional, mandatory, role-based and more recently attribute-based[1]. Discretional access control and mandatory access control model does not exhibit flexibility for a user to control the information flow. Role-based access control model has coarser-grained access structure than attributed based access control.

[*] 정회원, [**] 평생회원, 경북대학교 전자전기컴퓨터학부
(Kyungpook National University)
[***] 정회원, 경북대학교 산업전자공학과
(Kyungpook National University)
[ⓒ] Corresponding Author(E-mail: parkyh@knu.ac.kr)
※ 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(NRF-2012R1A1A4A01002603)
접수일자: 2013년5월1일, 수정완료일: 2013년8월19일

In a attributed based access control (ABAC), access decision is merely based on the attributes of users and the access structure given in resources or environment. ABAC model allows flexibility and scalability for large distributed file system. In general an ABAC mechanism usually deploy symmetric and public cryptographic schemes [2,3]. However, any public cryptography scheme only support one-to-one relation between a secret key and a ciphertext which is not compliance to the nature of ABAC model. Moreover, such kind access control solutions still rely on a trusted server and a secure storage.

Usually, an access control mechanism will protect a resource by dividing users into two groups: authorized users and unauthorized users and a user can be registered to several authorized users group of a resource. Therefore, an access control mechanism need an encryption scheme that provides complex relation between users (who own the secret keys) and resources (which protected by encryption). It was Sahai and Water[4] who the first proposed such kind of encryption. In their scheme, users and encrypted data has attributes. A user can decrypt data as long as she/he has enough attributes that matches with attributes in encrypted data. Futhermore, Goyal et al in [5] proposed a fine grained access control for attribute based encryption. Their scheme provide a mean to generate secret key with a fine grained access tree policy which built up by AND, OR and threshold gate. As access policy is attached in secret key while the ciphertext holds attributes we called such scheme as key-policy attributed based encryption (KP-ABE). Opposite to [5], Bethencourt et al [6] proposed a scheme which access policy is embedded in ciphertext rather than in secret key. Such scheme was named : ciphertext policy attributed based encryption CP-ABE.

Expressibility of the access structure is one of crucial features in a CP-ABE scheme. The fine grained access structure that proposed in [6-8] only allows monotonic access structure. Such limitation, makes some class of access structure can not be expressed in the CP-ABE scheme. For example, we want to set the authorized sets are only $\{x_1, x_2\}$ or $\{x_3, x_4\}$. No monotone access structure can express such requirement because the authorized sets only can be expressed in a non-monotonic boolean function:

$$(x_1 \wedge x_2 \wedge \neg x_3 \wedge \neg x_4) \vee (\neg x_1, \neg x_2 \wedge x_3 \wedge x_4).$$

Ostrovsky[9] developed an KP-ABE system that can be equipped with a non-monotone access structure, and as a consequence, a new gate which is the NOT gate is introduced in access policy. Since then, several CP-ABE systems allows non-monotonic access structure in their system[10-12]. In short, non-monotone access structures have more expressibility than monotone access structures.

There are many real applications of CP-ABE scheme most of them used CP-ABE to be provide access control service in a secure distributed data. For example, Huang and Verma applying CP-ABE to policy enforcementin a VANET system[13], Liang et al used CP-ABE scheme to provide access control in health information system[14], and Dongyoung et al used CP-ABE scheme to provide secure data retrieval over encrypted data in cloud storage[15].

In this paper, we construct a secure CP-ABE scheme where the policy can be constructed with non-monotone access structure (cf. the construction [6-8] that does not consider this treatment). Our construction has a different structure than [9] which is based on Sahai-Waters large universe construction [4]. In [10] all possible attributes must be mapped to three possible values, namely Non-Negated, Negated and Ignorable, which are included in the secret key. On the contrary, in our construction, the secret key length is in linear with the size of parameterized attribute set. In [11] the original scheme does not provide a CP-ABE scheme with a non-monotonic access structure. Eventhough[11] suggests a technique to transform their scheme to allow a non-monotonic access structure by doubling the size of attributes universe to include negated-attributes. Meanwhile, our CP-ABE scheme provides the 'real' NOT gate that does not double the size of attributes universe.

Our scheme provides more expressibility than [6-8] since our scheme introduces 'real' NOT gate in the access structures and keeps the attribute universe only include non-negated attributes which is a limitation in [9] and [10]. We provide the proof of our scheme in the generic bilinear model. We also compare the performance of our scheme with the existing schemes in the literature.

## Ⅱ. Backgrounds

To support our construction, we first present notation we used though out the paper, a formal definition of access structure, the ciphertext policy attribute-based encryption and linear secret sharing. Then, we review the definition of bilinear mapping and the related security assumptions.

### 1. Notation

Table 1 lists some important notations we used thoughout the construction and proof. The concrete meaning of notations will be further explained when the appear for the first time.

표 1. 기호들
Table 1. Notations.

| | |
|---|---|
| $Z_p$ | Integer field modulo $p$ |
| $\alpha,\beta,s,r_1,..,r_n,t$ | Integer in $Z_p$ |
| $x_1,x_2,...,x_n$ | Attributes $(x_i \in Z_p)$ |
| $U,X,Y$ | Set of attributes $X = x_1,...,x_n$ |
| $2^X$ | Powerset of $X$ |
| $\Gamma$ | Access structure $(\Gamma \subseteq 2^X)$ |
| $F$ | Boolean formula |
| $\Pi$ | Secret sharing |
| $\boldsymbol{M}$ | Matrix $\boldsymbol{M} \in Z_p^{l \times n}$ |
| $v$ | Vector $v \in Z_p^n$ |
| $G_1$ | Cyclic multiplicative group 1 |
| $g$ | Group generator for $G_1$ |
| $G_2$ | Cyclic multiplicative group 1 |
| $\hat{e}$ | Pairing map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ |
| $\hat{e}(g,g)$ | Group generator for $G_2$ |
| $b$ | Binary random $b \in \{0,1\}$ |
| $A$ | Adversary algorithm |
| $C$ | Challenger algorithm |

### 2. Access Structure

**Definition 1.** (Access Structure[16]). Let us define $U = \{x_1,...,x_n\}$ be a set of attributes. A collection $\Gamma \subseteq 2^U$ is monotone if $B \in \Gamma$ and $B \subseteq C$, implies $C \in \Gamma$. An access structure is a monotone collection $\Gamma$ of non-empty subsets of $2^U$. The sets in are called the authorized sets, and the sets not in $\Gamma$ are called the unauthorized sets.

The access structure $\Gamma$ contain all authorized sets of attributes. For example, let us assume that we have an attributes universe $U = \{x_1,x_2,x_3\}$ $\Gamma_1 = \{\{x_1,x_2\},\{x_1,x_3\},\{x_1,x_2,x_3\}\}$, $\Gamma_1$ is a monotonic access structure and can be expressed by a monotone boolean function: $F_1 = (x_1 \wedge x_2) \vee (x_1 \wedge x_3)$.

However, if the access structure $\Gamma_2 = \{\{x_1,x_2\},\{x_1,x_3\}\}$ then the access structure $\Gamma_2$ is non monotonic access structure and can only be expressed by a non monotone boolean function (the boolean function which includes NOT operator): $F_2 = (x_1 \wedge x_2 \wedge \neg x_3) \vee (x_1 \wedge \neg x_2 \wedge x_3)$. It is obvious that a non monotonic access structure has more expressibility than a monotonic access structure.

In our scheme, we used a non monotonic access boolean function to represent a non monotonic access structure. We require that the argument of NOT-gate (¬) should only be an attribute as shown in Fig. 1. We can use de Morgan law to place the NOT-gate in a leaf node instead in a non-leaf node in the access policy tree.. Therefore, in our scheme the attributes has two possibilities value: non-negated attribute $a_i$ and negated attribute $\neg a_i$.

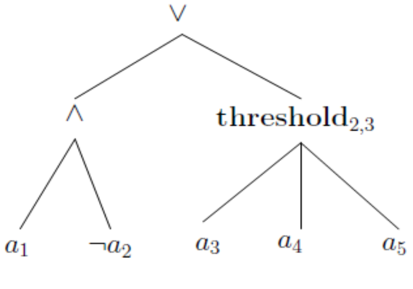

그림 1. 비단조 접근 방식의 예
Fig. 1. An Example of Non-Monotonic Access Policy.

## 3. Linear Secret Sharing Schemes

We use linear secret sharing schemes to generate a share for each attribute for an access structure $\Gamma$ define by a boolean function $F$.

**Definition 2.** (Linear Secret-Sharing Schemes (LSSS)[16]). A secret-sharing $\Pi$ over a set of attributes $\{x_1,\ldots,x_n\}$ is called linear (over $Z_p$) if

(1) The shares for each party form a vector over $Z_p$.

(2) There exists a matrix $\boldsymbol{M}$ with dimension $l \times n$ called the share-generating matrix for $\Pi$, For all $i=1,\ldots,l$, let the function $\rho$ defined the party labeling row $i$ as $\rho(i)$. When we consider a column vector $\boldsymbol{v}=(\boldsymbol{s},\boldsymbol{r_2},\ldots,r_n)$, where $s \in Z_p$ it the secret to be shared, and $r_2,\ldots,r_n \in Z_p$ are randommly chosen, then $\boldsymbol{Mv}$ is the vector of $l$ shares of the secret $s$ according to $\Pi$. The share $(\boldsymbol{Mv})_i$ belongs to party $\rho(i)$.

We require that the secret sharing $\Pi$ has *linear reconstruction* property, defined as follows: Suppose $\Pi$ is a secret sharing for an access structure $\Gamma$ define by a boolean function $F$ over a set of attributes $Y=\{y_1,..,y_l\}$. Let us defined $I=\{i:\rho(i)\in Y\}$. Then, we can find $\{\omega_i \in Z_p\}_{i\in I}$ in polynomial time such that $\sum_{i\in I}\omega_i\lambda_i = s$ where $\{\lambda_i \in Z_p\}_{i\in I}$ are valid shares for of any secret $s$.

The LSSS secret sharing scheme $\Pi$ is used for a set possible of monotonic access structure. To realize non-monotonic access structures with the LSSS $\Pi$, we define for each access structure $\Gamma$ over an attributes set $Y=\{\hat{x}_1,..,\hat{x}_l\}$ has the following properties: An attribute $\hat{x}_i \in Y$ is either a non-negated attribute $\hat{x}_i = x_i$, or a negated $\hat{x}_i = \neg x_i$.

## 4. CP-ABE

The CP-ABE scheme $\Sigma$ is defined over a set of attributes $U=x_1,\ldots,x_N$ and a plaintext space $M$. and contains of four algorithms: $setup$, $keygen$, $encrypt$, and $decrypt$.

- $(pk,msk)\leftarrow setup(k,d)$. Where $k$ is a security parameter, $d$ is an universe attribute description, $pk$ is a set of public parameters, and $msk$ is a set of master keys.
- $SK_X \leftarrow keygen(pk,msk,X)$. Where $X \subseteq U$ is a set of attributes, and $SK_X$ is a secret key that parameterized by $X$.
- $CT_\Gamma \leftarrow encrypt(pk,m,\Gamma)$. Where $m \in M$ is a plaintext, $\Gamma \subseteq 2^U$ is an access structure, and $CT_\Gamma$ is a ciphertext parameterized by the access structure $\Gamma$.
- $m|\perp \leftarrow decrypt(pk,SK_X,CT_\Gamma)$. The decryption outputs a message $m$ or a random $\perp$.

**Correctness.** A CP-ABE scheme $\Sigma$ over a set of attributes $U$ and a plaintext space $M$, the scheme must satisfy the following correctness property:

$$\forall\ X \subseteq U, \forall\ \Gamma \subseteq 2^U,\quad \forall\ m \in M:$$
$$(pk,msk)\leftarrow setup(k),$$
$$SK_X \leftarrow keygen(pk,msk,X),$$
$$CT_\Gamma \leftarrow encrypt(pk,m,\Gamma),$$
if $X \in \Gamma$ ( $X$ is an authorizes set in $\Gamma$)
then $m \leftarrow decrypt(pk,SK_X,CT_\Gamma)$.

In Figure 2, we present typical use of CP-ABE

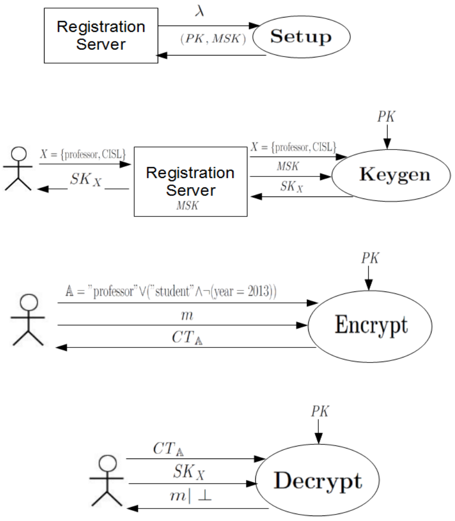

그림 2. CP-ABE 방식의 전형적인 사용
Fig. 2. Typical Use of a CP-ABE scheme.

scheme in an access control for a secure distributed file application. The access control system contains 3 parties: the registration server, encryptor and decryptor. The registration server, at first, should run setup algorithm: $(pk, msk) \leftarrow setup(k, d)$ from the CP-ABE scheme $\Sigma$ and publishes the public parameters $pk$ and keeps the master key $msk$. The decryptor must ask his/her secret key by giving a set of attributes to the registration server, in Figure 2, the attribute set is $X = \{professor, CISL\}$, in order to generate his/her secret key $SK_X$. Next, the encryption when he/she wants to encrypt a plaintext $m$ in order to protect its access, he/she should give an access policy to the encryption algorithm, in Figure 2, the access policy is $\Gamma = professor \vee (student \wedge \neg(year = 2013))$, to produce a ciphertext $CT_\Gamma$. When a decyrptor who owns $SK_X$ wants to recover a ciphertext $CT_\Gamma$, then the decryption algoritm will check whether $X$ satisfying the access policy $\Gamma$ or not. If $X$ satisfy $\Gamma$ then the plaintext is recovered. In Figure 2, $X = \{professor, CISL\}$ is satisfying $\Gamma = professor \vee (student \wedge \neg(year = 2013))$ therefore the decryptor can recover the plaintext $m$. However, if $X = \{student, year = 2013\}$ then the decryptor can not recover the plaintext $m$.

We follow CP-ABE security model based on indistinguishable game under chosen-plaintext attacker $A$ (CPABE-IND-CPA) as follows[6]:

- **Setup**. The challenger $C$ runs the $setup$ algorithm and gives the public parameters $pk$ to the adversary $A$.
- **Phase 1**. The adversary $A$ makes repeated private keys corresponding to arbitrary sets of attributes $X_1, \ldots, X_{q_1}$.
- **Challenge**. The adversary $A$ submits two equals length messages $m_0$ and $m_1$ to the challenger $C$. In addition the adversary gives a challenge non-monotone access structure $\Gamma^*$ given that none of the sets $X_1, \ldots, X_{q_1}$ from Phase 1 satisfy the challenge access structure $\Gamma^*$. The challenger $C$ flips a random coin $b \leftarrow \{0, 1\}$ and call $CT_{\Gamma^*} \leftarrow encrypt(pk, m_b, \Gamma^*)$ and gives $CT_{\Gamma^*}$ to $A$
- **Phase 2**. Phase 1 is repeated with the restriction that none of sets of attributes $X_{q_1}, \ldots, X_q$ satisfy the access structure corresponding to the challenge access structure $\Gamma^*$.
- **Guess**. The adversary $A$ utputs a guess $b'$ of $b$.

The advantage of an adversary $A$ in this game is defined as

$$\boldsymbol{Adv}_{\Sigma, A}^{CPABE-IND-CPA} = \left| \Pr[b = b'] - \frac{1}{2} \right| \quad (1)$$

This model can be extended to handle chosen-chipertext attacks by allowing for decryption queries in Phase 1 and Phase 2.

**Definition 3.** (Secure CP-ABE Scheme [6]). A CP-ABE scheme $\Sigma$ is secure if all PPT adversary $A$ has at most a negligible advantage in CPABE-IND-CPA game.

### 5. Bilinear Maps

We present a few facts about groups and the bilinear map. Let us define a group generator $(G_1, G_2, \hat{e}) \leftarrow \boldsymbol{gen}(k)$ that produces two cyclic groups $G_1$ and $G_2$ of prime order $p$. and a bilinear map $\hat{e}: G_1 \times G_1 \rightarrow G_2$. The bilinear map $\hat{e}$ has the following properties:

- Bilinearity: for all $g, h \in G_1$ and $\alpha, \beta \in Z_p$, we have $\hat{e}(g^\alpha, h^\beta) = \hat{e}(g, h)^{\alpha\beta}$
- Non-degeneracy: there exist $g \in G_1$ such that $\hat{e}(g, g) \neq 1$.

We require that the group operation in $G_1$ and $G_2$, and the bilinear map $\hat{e}$ are efficiently computable.

### 6. Generic Bilinear Group Model.

Our proof use the generic bilinear model used in [6, 17] together with the random oracle model [18] to argue that no efficient adversary that acts generically on the groups that underlays our scheme and can break the security of our scheme with any reasonable probability.

**Definition 4.** (The generic bilinear group model [17]). Let us define two random encoding $\psi_1, \psi_2 : Z_p \rightarrow \{0,1\}^m$, where $m > 3\log(p)$. We denote for $i = 1,2$ $G_i = \{\psi_i(x) : x \in Z_p\}$. We are given oracles to compute group operations in $G_1$ and $G_2$, and bilinear map $\hat{e}$. We refer $\left(G_1, G_2, \hat{e}\right)$ as a generic bilinear group model.

## Ⅲ. Construction

In the rest of the paper, $\Delta_{i,S}(x)$ denotes the Lagrange coefficient for $x, i \in Z_p$ and a set $S$ of integers in $Z_p$. Then, Lagrange coefficient can be computed as follows.

$$\Delta_{i,S}(x) = \prod_{i \in S, j \neq i} \frac{x-j}{i-j} \tag{2}$$

We additionally employ a hash function $H : Z_p \rightarrow G_1$. We assume that each attribute already been assigned to an arbitrary element in $Z_p$.

Our proposed CP-ABE scheme contains 4 algorithm:

### (1) Setup algorithm.

$(pk, msk) \leftarrow setup(k,d)$: the setup algorithm executes as follows. It chooses $d \in Z_p$ the number of attributes in a secret key. Then, it runs $(G_1, G_2, \hat{e}) \leftarrow gen(k)$, chooses a generator $g \in G_1$, selects randomly $\alpha, \beta, a_1, .., a_d \leftarrow Z_p$ and sets a polynomial $q(x) = a_d x^d + \ldots + x + \dfrac{1}{\beta}$. Finally the public parameters $pk$ is published as

$$PK = \left\{G_1, G_2, \hat{e}, g, \hat{e}(g,g)^{\alpha}, g^{\beta}, V(x)\right\} \tag{3}$$

where $V(x) : Z_p \rightarrow G_1$ is public function defined as

$$V(x) = g^{q(0)\Delta_{0,I}(x)} \prod_{i=1}^{d-1} g^{q(i)\Delta_{i,I}(x)} \tag{4}$$

where $I = \{0, 1, \ldots, d-1\}$. The master key is defined as

$$msk = \{g^{\alpha}, \beta\} \tag{5}$$

### (2) Key generation algorithm.

$SK_X \leftarrow keygen(pk, msk, X)$: Given a set of attribute $X = \{x_1, \ldots, x_d\}$ where for all $\forall\ x \in X, x \in Z_p$, the key generation algorithm chooses randomly $r, r_1, \ldots, r_d \leftarrow Z_p$. Then, it computes the secret key as

$$SK_X = \left\{ \begin{matrix} X, D_1 = (g^{\alpha} g^{r})^{\frac{1}{\beta}}, D_2 = (g^{\beta})^{r} \\ \left\{ \begin{matrix} D_{3,i} = g^{r_i}, \\ D_{4,i} = g^{r} H(x_i)^{r_i}, \\ D_{5,i} = V(x_i)^{\beta r} \end{matrix} \right\}_{i = 1, .., d} \end{matrix} \right\} \tag{6}$$

### (3) Encryption algorithm.

$CT_{\Gamma} \leftarrow encrypt(pk, m, \Gamma)$. Given a message $m \in G_2$ and a non monotonic access structure $\Gamma$ associated with a linear secret sharing $\Pi$ with share generating matrix $\boldsymbol{M} \in Z_p^{l \times n}$. Let $\hat{Y} = \{\rho(i)\}, \forall i \in \{1, \ldots, 1\}$ be a set of non-negated and negated attributes defining the access structure. First, the encryption algorithm chooses randomly $s, s_2, \ldots, s_n \leftarrow Z_p$ and sets a column vector $\boldsymbol{v} = (s, s_2, \ldots, s_n)$. Then, for each $Y = \{\rho(i)\}, \forall i \in \{1, \ldots, 1\}$ compute share $\lambda_i = (\boldsymbol{Mv})_i$. Let us denote $I = \{1, .., l\}$, and $Y \subseteq \hat{Y}$ contains only non-negated attributes in $\hat{Y}$ then the ciphertext is computed as follows:

$$CT_{\Gamma} = \left\{ \begin{matrix} \Gamma, E_1 = m\,\hat{e}(g,g)^{\alpha s}, E_2 = (g^{\beta})^{s}, \\ \left\{E_{3,i} = g^{\lambda_i}\right\}_{\forall i \in I} \\ \left\{E_{4,i} = H(y_i)^{\lambda_i}\right\}_{\forall y_i \in Y'} \\ \left\{E_{4,i} = V(y_i)^{\lambda_i}\right\}_{\forall \neg y_i \in \hat{Y} - Y} \end{matrix} \right\} \tag{7}$$

### (4) Decryption algorithm.

$decrypt(pk, SK_X, CT_{\Gamma})$. Given a secret key $SK_X$ parametrized by a set of attributes $X$ and a ciphertext $CT_{\Gamma}$ parameterized by an access structure

$\Gamma$ with share-generating matrix $\boldsymbol{M} \in Z_p^{l \times n}$ and $Y = \{\rho(i)\}, \forall\ i \in \{1,...,l\}$ be a set of non-negated and negated attributes defining the access structure. The decryption algorithm does the following: First, it checks whether $X \in \Gamma$, if $X \notin \Gamma$ then returns $\perp$. Otherwise, we have the following conditions: (1) For each satisfied non-negated attribute $\hat{y_i}$ in $Y$ that is $\hat{y_i} = y_i$, there must be a match $y_i = x_j \in X$ (2) For each satisfied negated attribute $\hat{y_i}$ in $Y$ that is $\hat{y_i} = \neg y_i$ we require $\forall x_j \in X$ satisfied $y_i \neq x_j$.

Let us define $\hat{I}$ as a set of satisfied index in $Y$, the linear secret sharing scheme $\Pi$ yields a set of coefficients $\Omega = \{\omega_i\}_{i \in \hat{I}}$ such that $\sum_{i \in \hat{I}} \omega_i \lambda_i = s$. Next, for each $i \in \hat{I}$:

If $\hat{y_i} \in Y$ is a non-negated attribute $\hat{y_i} = y_i$ then $y_i = x_j \in X$, do the following computation:

$$Z_i = \left( \frac{\hat{e}(D_{4,j}, E_{3,i})}{\hat{e}(D_{3,j}, E_{4,i})} \right)^{\omega_i} = \left( \frac{\hat{e}(g^r H(x_j)^{r_j}, g^{\lambda_i})}{\hat{e}(g^{r_j}, H(y_i)^{\lambda_i})} \right)^{\omega_i} = \hat{e}(g,g)^{r\lambda_i\omega_i} \qquad (8)$$

If $\hat{y_i} \in Y$ is a negated attribute $\hat{y_i} = \neg y_i$ then $y_i \notin X$. Let $\hat{X} = X \cup y_i$ and $I = \{1,...,d\}$, the decryption algorithm do the following computation:

$$\begin{aligned} Z_i &= \left( \hat{e}\Big( \prod_{\forall j \in I} (D_{5,j})^{\Delta_{x_j,\hat{X}}(0)}, E_{3,i} \Big) \hat{e}(D_2, E_{4,i})^{\Delta_{y_i,\hat{X}}(0)} \right)^{\omega_i} \\ &= \left( \hat{e}\Big( \prod_{j \in I} (V(x_j)^{\beta r \Delta_{x_j,\hat{X}}(0)}, g^{\lambda_i} \Big) \hat{e}(g^{\beta r}, V(y_i)^{\lambda_i})^{\Delta_{y_i,\hat{S}}(0)} \right)^{\omega_i} \\ &= \hat{e}(g,g)^{r\beta\omega_i\lambda_i \sum_{x \in \hat{X}} q(x)\Delta_{x,\hat{S}}(0)} \\ &= \hat{e}(g,g)^{r\beta\omega_i\lambda_i \frac{1}{\beta}} \\ &= \hat{e}(g,g)^{\omega_i\lambda_i r} \end{aligned} \qquad (9)$$

At the end, the plaintext is obtained by computing:

$$\begin{aligned} \frac{E_1 \prod_{\forall i \in \hat{I}} Z_i}{\hat{e}(D_1, E_2)} &= \frac{m\,\hat{e}(g,g)^{\alpha s} \hat{e}(g,g)^{r \sum_{\forall i \in \hat{I}} \lambda_i \omega_i}}{\hat{e}(g^{(\alpha+r)/\beta}, g^{\beta s})} \\ &= \frac{m\,\hat{e}(g,g)^{(\alpha+r)\,\mathrm{s}}}{\hat{e}(g,g)^{(\alpha+r)\,\mathrm{s}}} \\ &= m \end{aligned} \qquad (10)$$

## Ⅳ. Proof of Security

In this section, we present the proof of our scheme based on generic bilinear model [6, 17] and the random oracle model [18].

**Theorem 1.** Let us define $\psi_1, \psi_2, G_1, G_2$ be defined as generic bilinear group model. For any adversary $A$, let $q$ be a bound on the total number of group elements it receives from queries it makes to the oracles for the hash function $H$, $G_1$, $G_2$ and the bilinear map $\hat{e}$ and from its interaction with the CP-ABE security game. Then we have that the advantage of the adversary in the CP-ABE security game is $O(q^2/p)$.

**Proof.** Let us write $g = \psi_1(1)$, $g^x$ to denote $\psi_1(x)$, and $\hat{e}(g,g)^y$ to denote $\psi_2(y)$. We build an algorithm challenger $C$ in CPABE-IND-CPA indistinguishable-game with adversary $A$. When the challenger $C$ or the adversary $A$ calls for evaluation of hash function $H$ on any element $x \in Z_p$, a new random $t_x \in Z_p$ is selected unless it already been chosen, and the oracle provides $g^{t_x}$ as the respond to $H$(x). The simulation proceeds as follows:

- **Setup.** The challenger $C$ selects non-zero $\alpha, \beta \leftarrow Z_p$. randomly and sets public parameters as Equation 3 and sends $pk$ to the adversary $A$.
- **Phase 1.** In phase 1, the adversary $A$ makes $q_1$ secret key queries. For each query, when the the adversary $A$ makes $j$-th secret key query for a set of attributes $X_j$. The challenger $C$ responds by selecting a new random values $r^{(j)}, r_1^{(j)}, ...., r_d^{(j)}$ and sets $SK_{X_j}$ as Equation 6, where $r = r^{(j)}, r_1 = r_1^{(j)}, ...., r_d = r_d^{(j)}$ and sends $SK_{X_i}$ to the adversary $A$.
- **Challenge.** The adversary $A$ submits two equals length messages $m_0$ and $m_1$, and a challenge non-monotone access structure $\Gamma^*$ associated with a linear secret sharing $\Pi$ with

share generating matrix $\boldsymbol{M} \in Z_p^{l \times n}$ and $Y = \{\rho(i)\}, \forall\ i \in 1,...,l$ be a set of non-negated and negated attributes defining the access structure., given that none of the sets $X_1,...,X_{q_1}$ from Phase 1 satisfy the challenge access structure $\Gamma^*$. The challenger $C$ does the following:

(a) Selects $s, \mu_2, .., \mu_l, \theta \leftarrow Z_p$.

(b) $\forall i \in \{1,...,l\}$, generate share for party $\rho(i)$, $\lambda_i = (\boldsymbol{Mv})_i$ where $\boldsymbol{v}$ is a column vector $(s, \mu_2, .., \mu_l)$.

(c) Flips a random coin $b \leftarrow \{0,1\}$. If $b = 0$ sets $E_1 = \hat{e}(g,g)^\theta$, otherwise $E_1 = m_1 \hat{e}(g,g)^\theta$ and constructs other elements of $CT_{\Gamma^*}$ as Equation 7.

(d) Sends $CT_{\Gamma^*}$ to the advesary $A$.

- **Phase 2.** Phase 1 is repeated with the restriction that none of sets of attributes $X_{q_1},...,X_q$ satisfy the access structure corresponding to the challenge access structure $\Gamma^*$.
- **Guess.** The adversary outputs a guess $b'$ of $b$.

Now, we are analyzing the game. When $b = 0$, the simulation sets $E_1 = \hat{e}(g,g)^\theta$ (a random value from $G_2$) by theorem given by [14] the randomness of the choice variable is $1 - O(q^2/p)$. Therefore, the adversary advantage is $O(q^2/p)$.

When $b = 1$, the simulation sets $E_1 = m_1 \hat{e}(g,g)^{\alpha s}$. The adversary can break the ciphertext if it can construct a query in the form $\hat{e}(g,g)^{\gamma\alpha s}$ where $\gamma$ is a constant. However, we argue that the adversary can *never* constructs such expression. From the simulation, the only way for the adversary to construct $e(g,g)^{\gamma\alpha s}$ by pairing $(g^\alpha g^{r^{(j)}})^{\frac{1}{\beta}}$ and $g^{\beta r^{(j)}}$ which result $e(g,g)^{\alpha s} e(g,g)^{s r^{(j)}}$. In this way, the adversary could create a query of $e(g,g)$ containing $\gamma\alpha s + \sum_{j \in T} \gamma_i s r^{(j)}$. Therefore, in order to obtain a query in the form $\gamma\alpha s$, the adversary $A$ must cancel the term $\gamma_i s r^{(j)}$. By analyzing possible of queries type (by pairing all of element in $CT_{\Gamma^*}$ and all $SK_{X_j}$), the only possible of query types that the adversary $A$ can construct to cancel the term is by pairing $g^{\lambda_{i'}}$ with other element in $SK_{S_j}$ which exponential containing $r^{(j)}$. Futhermore, we should consider the following case:

**Case 1.** (Negative non-negated attribute). For $x_{i,j} \in X_j,\ \forall\ y_k \in Y: y_k \neq x_{i,j}$. The adversary $A$ can have a query in $G_2$: $\lambda_k r^{(j)} + \lambda_k t_i r_i^{(j)}$, however the adversary $A$ does not have a way to cancel out $\lambda_k t_i r_i^{(j)}$.

**Case 2.** (Negative negated attribute). For $x_{i,j} \in X_j$, $\exists\ \neg y_k \in Y: y_k = x_{i,j}$. The adversary $A$ can have a query in $G_2$: $\beta\lambda_k r^{(j)}$ for $\forall\ y_k \in Y$. However, the adversary could not cancel $\beta$ from $\beta\lambda_k r^{(j)}$ since it is a discrete logarithm problem in $G_2$.

**Case 3.** (Positive non-negated). For $x_{i,j} \in X_j$, $\exists\ y_k \in Y: y_k = x_{i,j}$. The adversary $A$ can have $\lambda_k r^{(j)} + \lambda_k t_i r_i^{(j)}$ and cancels $\lambda_k t_i r_i^{(j)}$, to have $\lambda_k r^{(j)}$. However, since $X_j \not\in \Gamma^*$, $\lambda_k r^{(j)}$ is useless since the adversary cannot reconstruct $s$. (There must be a $x_{i,j} \in X_j$, satisfy case 1 or case 2).

**Case 4.** (Positive negated). For $\neg y_k \in Y, \forall\ x_{i,j} \in X: x_{i,j} \neq y_k$. In this case, the adversary can cancel $\beta$ from $\beta\lambda_k r^{(j)}$ by interpolating using Lagrange coefficient for $\widehat{X_j} = X_j \cup y_k$. However, again since $X_j \not\in \Gamma^*$, $\lambda_k r^{(j)}$ is useless since the adversary $A$ cannot reconstruct $s$. (There must be a $s_{i,j} \in S_j$, satisfy case 1 or case 2).

Therefore the adversary's query of $e(g,g)$ cannot be in the form $\gamma\alpha s$. This completes our proof.

## V. Comparisons

In this section, we present a comparison between our scheme and the existing schemes in the literature. Firstly, we would like to compare our work to [8~9] as they also constructed CP-ABE with

표 2. 기존의 CP-ABE 방식들과 제안한 방식의 비교
Table 2. Comparisons of Our Scheme to Existing CP-ABE Schemes

| | Ours | LC-CP-ABE [11] | BT-CP-ABE [6] | OT-CP-ABE [12] |
|---|---|---|---|---|
| Monotonic | Non | Non | Monotonic | Non |
| Security | Full | Selective | Full | Full |
| $\|pk\|$ | $(2+d)\|G_1\|$ $+\|G_2\|$ | $3n\|G_1\|$ $+\|G_2\|$ | $2\|G_1\|$ $+\|G_2\|$ | $3(n+1)\|G_1\|$ $+\|G_2\|$ |
| $\|CT_\Gamma\|$ | $(2l+1)\|G_1\|$ $+\|G_2\|$ | $(n+1)\|G_1\|$ $+\|G_2\|$ | $(2l+1)\|G_1\|$ $+\|G_2\|$ | $3(l+3)\|G_1\|$ $+\|G_2\|$ |
| $\|SK_X\|$ | $(3d+2)\|G_0\|$ | $(2n+1)\|G_0$ | $(2d+1)\|G_0\|$ | $(4d+3)\|G_0\|$ |
| $T_{dec}$ | $(2m+1)\ T_p$ | $n\,T_p$ | $(2m+1)\ T_p$ | $(7m+2)\ T_p$ |

non-monotonic access structure. In this comparison, we denote these work as LC-CP-ABE and OT-CP-ABE. Finally, we also include the work from [6], which was the first CP-ABE construction. We denote this work as BT-CP-ABE.

Comparing to BT-CP-ABE, from [6] we can see from Table 2 that our scheme allows non-monotonic access structure to be used in creating ciphertexts. Where in [6] still problematic. The non-monotonicity of our scheme gives more expressibility in defining access policy than [6]. Our scheme includes the NOT-gate and still maintains AND, OR and threshold-gate which is also included in LC-CP-ABE from [11] and OT-CP-ABE from [12]. However, compare to [6], our scheme requires more spaces in key or ciphertext length and time for procedure executions.

In regards of space requirement for public parameters $|pk|$, our scheme is in linear function of $d$ (the maximum size of set of attributes in secret key), while LC-CP-ABE and OT-CP-ABE is in linear function of $n$ (number of possible attributes). Therefore, our proposed scheme can be used for large universe attributes which problematic in LC-CP-ABE and OT-CP-ABE. For space requirement of a ciphertext $|CT_\Gamma|$ and a secret key $|SK_X|$, our proposed scheme and OT-CP-ABE are in linear function of $l$ (number of attributes in for $|CT_\Gamma|$, and linear function of $d$ (number of attributes in $S$). However, according to Table 2 our proposed scheme has less memory requirement than OT-CP-ABE for storing a secret key $SK_X$ or a ciphertext $CT_\Gamma$.

In regards to the computation cost, we assume costliest computation is pairing computation $T_p$ in decryption algorithm. The number of pairing in our proposed scheme and OT-CP-ABE are in linear function of $m$ (number of matching attributes) but ours has lower number of pairing . While LC-CP-ABE is in linear function of $n$ (number of possible atttributes). It clearly our scheme and OT-CP-ABE will outperform LC-CP-ABE by the length of key or ciphertext and the cost of all procedures if $n > 2d+1$.

## Ⅵ. Conclusions

We presented Ciphertext-Policy Attribute-Based Encryption system that supports the expression of non-monotonic access controls in ciphertext policy. We achieve this through the combination of revocation methods and general linear secret sharing scheme. We proved our system in generic bilinear group and random oracle. In addition, the performance of our scheme is more favorable than existing CP-ABE with non-monotonic access controls. A future work in the line of this work would be the construction of CP-ABE which is proven secure under standard and non-interactive assumption.

## REFERENCES

[1] R. S. Sandhu and P. Samarati, “Access Control: Principles and Practice.”, *Communications Magazine, IEEE*, vol. 32, no. 9, pp. 40 - 48, 1994.

[2] A. Kapadia, P. P. Tsang, and S. W. Smith. "Attribute-based publishing with hidden credentials and hidden policies." *in Proceedings of The 14th Annual Network and Distributed System Security Symposium (NDSS)*, pp. 179-192, 2007.

[3] M. Pirretti, P. Traynor, P. McDaniel and B. Waters, "Secure attribute-based systems." in *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 99-112, 2006.

[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption", *EUROCRYPT, Lecture Notes in Computer Science*, vol 3494, pp. 457-473. Springer, 2005.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data.” in *Proceedings of the 13th ACM conference on Computer and communications security*, CCS ’06, (New York, NY, USA), pp. 89 - 98, ACM, 2006.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption." in *IEEE Symposium on Security and Privacy*, pp. 321-334, IEEE Computer Society, 2007.

[7] L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker, “*Efficient and provable secure ciphertext-policy attribute-based encryption schemes.*” in Proceedings of the 5th International Conference on Information Security Practice and Experience, ISPEC ’09, (Berlin, Heidelberg), pp. 1 - 12, Springer-Verlag, 2009.

[8] B. Waters, “Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization.” in *Proceedings of the 14th international conference on Practice and theory in public key cryptography conference on Public key cryptography*, PKC’11, (Berlin, Heidelberg), pp. 53 - 70, Springer-Verlag, 2011.

[9] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures." in *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 195-203, 2007.

[10] Goyal, V., Jain, A., Pandey, O., & Sahai, A.. "Bounded ciphertext policy attribute based encryption". In *Automata, Languages and Programming*, pp.579-591, Springer Berlin Heidelberg, 2008.

[11] L. Cheung and C. Newport, “Provably secure ciphertext policy ABE,” in *Proceedings of the 14th ACM conference on Computer and communications security*, CCS ’07, (New York, NY, USA), pp. 456 - 465, ACM, 2007.

[12] T. Okamoto and K. Takashima, “Fully secure functional encryption with general relations from the decisional linear assumption.” in *Advances in Cryptology CRYPTO 2010* (T. Rabin, ed.), vol. 6223 of Lecture Notes in Computer Science, pp. 191 - 208, Springer Berlin, Heidelberg, 2010.

[13] Huang, Dijiang, and Mayank Verma, "ASPE: attribute-based secure policy enforcement in vehicular ad hoc networks." *Ad Hoc Networks*, Vol 7, no. 8, pages 1526-1535, 2009.

[14] Liang, X., Barua, M., Lu, R., Lin, X., & Shen, X. S.. "Healthshare: Achieving secure and privacy-preserving health information sharing through health social networks.", *Computer Communications*, vol 35, no 15, pp. 1910-1920, 2012.

[15] Koo, D., Hur, J., & Yoon, H. "Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage.", *Computers & Electrical Engineering*, vol 39, no 1, pp 34-46, 2013.

[16] A. Beimel, *Secure schemes for secret sharing and key distribution*. PhD thesis, Israel Institute of Technology, 1996.

[17] V. Shoup. "Lower bounds for discrete logarithms and related problems". In *EUROCRYPT*, pp. 256 - 266, 1997.

[18] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *ACM conference on Computer and Communications Security* (ACM CCS), pp. 62 - 73, 1993.

## 저자소개

리프키 사디킨(정회원)
1999년 Gadjah Mada 대학교 전기공학과 학사
2004년 Indonesia 대학교 컴퓨터공학과 석사
2009년～현재 경북대학교 전자전기컴퓨터학부 박사과정
<주관심분야 : 정보보호, 네트워크보안>

문 상 재(평생회원)
1972년 서울대학교 공업교육(전자전공)과 학사
1974년 서울대학교 전자공학과 공학석사
1984년 미국 UCLA 전기공학과 공학박사
1984년～1985년 미국 UCLA 포스트닥터
1984년～1985년 미국 OMNET 회사 컨설턴트
1974년～2013년 경북대학교 IT대학 전자공학부 교수
2002년～2013년 한국정보보호학회 명예회장
<주관심분야 : 무선통신, 네트워크보안, 암호학>

박 영 호(정회원)-교신저자
1989년 경북대학교 전자공학과 학사
1991년 경북대학교 전자공학과 석사
1995년 경북대학교 전자공학과 박사
1996년～2008년 상주대학교 전자전기공학부 교수
2003년～2004년 Oregon State Univ. 방문교수
2008년～현재 경북대학교 산업전자공학과 교수
<주관심분야 : 정보보호, 네트워크보안, 모바일 컴퓨팅>